APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/646,938	08/22/2003	Takaharu Nakamura	FUSA 20.586	1772

26304	7590	11/02/2006

KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER
FOX, BRYAN J

ART UNIT	PAPER NUMBER
2617	

DATE MAILED: 11/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>09 August 2006</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5 and 7-15* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5 and 7-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August

9, 2006 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating
      obviousness or nonobviousness.

Claims 1 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Dent et al in view of Tsubakiyama (US005544245A).

Regarding **claim 1**, Dent et al disclose bi-directional authentication between a

mobile station and a base station, so that it is not only the base station that requires the

identity of the mobile station, but the mobile station that requires the identity of the base

station (see column 1, line 67 – column 2, line 7), which reads on the claimed, "mobile

terminal in a mobile communication system for authenticating a communicating party

when communication is performed between the mobile terminal and a device on the

side of a network." After the base station authenticates the mobile station, the base

station forms a response signal from a further random number RAND2 and form the

personal identification number PIN of the mobile, this number being known in the base

station and this is sent to the mobile station. The mobile station forms a value of

RESP2 from its PIN and the received number RAND2 and compares this formed value

with the received RESP2. If the two values coincide, the method proceeds (see column

3, lines 4-34 and figure 2), which reads on the claimed, "authentication processing

means which, when a request signal requesting operation execution is received from a

network device, is for executing authentication processing to check whether said

request signal is a request signal from an authorized network device; and operation

execution means for executing an operation that is in accordance with said request

signal only if authentication that the network device is an authorized network device is

obtained," wherein the request signal requesting operation execution is the random

number sent from the base station requesting a connection. A random number is sent

from the BS and the MS responds. The BS calculates and compares the response,

then forms another response and sends it to the MS. The MS calculates a response

and compares and forms another response to the BS and sends it (see figure 2), which reads on the claimed, "means for storing an identifier and key information of a mobile terminal... an authentication operation unit for executing a prescribed authentication operation using said key information and random number; an authentication request signal transmitter for creating an authentication request signal transmitter for creating an authentication request signal, which includes said terminal identifier and random number, and sending this signal to the network device; a receiver for receiving an authentication result, which has been obtained by an authentication operation performed on the network side, from the network device; and a comparator for comparing the authentication result computed by the mobile terminal and the authentication result sent form the network device; and said operation execution means executes the operation that is in accordance with said request signal upon deciding that the network device is an authorized network device when the compared results agree." Dent et al fail to expressly disclose that the mobile terminal includes a random number generator.

In a similar field of endeavor, Tsubakiyama discloses a system where the mobile terminal generates a random number (see column 4, lines 38-42).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Dent et al with Tsubakiyama to include the above random number generator at the mobile unit in order to greatly contribute to future network security while the extra burden on the system is very slight (see column 5, lines 17-34).

Regarding **claim 5**, Dent et al disclose bi-directional authentication between a

mobile station and a base station, so that it is not only the base station that requires the

identity of the mobile station, but the mobile station that requires the identity of the base

station (see column 1, line 67 – column 2, line 7), which reads on the claimed, "mobile

communication system for authenticating a communicating party when communication

is performed between a mobile terminal and a device on the side of a network." After

the base station authenticates the mobile station, the base station forms a response

signal from a further random number RAND2 and form the personal identification

number PIN of the mobile, this number being known in the base station and this is sent

to the mobile station. The mobile station forms a value of RESP2 from its PIN and the

received number RAND2 and compares this formed value with the received RESP2. If

the two values coincide, the method proceeds (see column 3, lines 4-34 and figure 2),

which reads on the claimed, "authentication processing means which, when a signal

requesting execution of a prescribed operation has been received from a network

device, is for sending an authentication request signal to the network device in order to

determine whether said request signal is a request signal from an authorized network

device; performing an authentication operation; and comparing result of this

authentication operation with result of an authentication operation sent from the network

device; and operation execution means for executing an operation that is in accordance

with said request signal only if authentication that the network device is an authorized

network device is obtained; and said network device includes an authentication

operation unit for executing an authentication operation based upon an authentication

request signal received from said mobile terminal based upon an authentication request signal received from said mobile terminal, and sending result of this authentication operation to the mobile terminal," wherein the request signal requesting operation execution is the random number sent from the base station requesting a connection. A random number is sent from the BS and the MS responds. The BS calculates and compares the response, then forms another response and sends it to the MS. The MS calculates a response and compares and forms another response to the BS and sends it (see figure 2), which reads on the claimed, "means for storing an identifier and key information of a mobile terminal... an authentication operation unit for executing a prescribed authentication operation using said key information and random number; an authentication request signal transmitter for creating an authentication request signal transmitter for creating an authentication request signal, which includes said terminal identifier and random number, and sending this signal to the network device; a receiver for receiving an authentication result, which has been obtained by an authentication operation performed on the network side, from the network device; and a comparator for comparing the authentication result computed by the mobile terminal and the authentication result sent form the network device; and said operation execution means executes the operation that is in accordance with said request signal upon deciding that the network device is an authorized network device when the compared results agree." Dent et al fail to expressly disclose that the mobile terminal includes a random number generator.

In a similar field of endeavor, Tsubakiyama discloses a system where the mobile

terminal generates a random number (see column 4, lines 38-42).

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to modify Dent et al with Tsubakiyama to include the above random

number generator at the mobile unit in order to greatly contribute to future network

security while the extra burden on the system is very slight (see column 5, lines 17-34).

Claims 4 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Dent et al in view of Hayashi et al.

Regarding **claim 4**, Dent et al disclose bi-directional authentication between a

mobile station and a base station, so that it is not only the base station that requires the

identity of the mobile station, but the mobile station that requires the identity of the base

station (see column 1, line 67 – column 2, line 7), which reads on the claimed, "network

device in a mobile communication system for authenticating a network device by

comparing, at a mobile terminal, authentication results computed by respective ones of

the mobile terminal and network device when communication is performed between

these two devices." After the base station authenticates the mobile station, the base

station forms a response signal from a further random number RAND2 and form the

personal identification number PIN of the mobile, this number being known in the base

station and this is sent to the mobile station. The mobile station forms a value of

RESP2 from its PIN and the received number RAND2 and compares this formed value

with the received RESP2. If the two values coincide, the method proceeds (see column

3, lines 4-34 and figure 2), which reads on the claimed, "means for sending a signal, which requests that a mobile terminal execute a prescribed operation, to said mobile terminal... a receiver for receiving, from the mobile terminal that has received said request signal, an authentication request signal that includes the identifier and random number of said mobile terminal," and, "an authentication operation unit for executing an authentication operation," and, "a transmitting unit for transmitting the authentication result to the mobile terminal." Dent et al fails to disclose the use of a table for storing correspondence between an identifier and key information of a mobile terminal and a key-information acquisition unit for acquiring key information, which corresponds to the received identifier of the mobile terminal, from said table.

In a similar field of endeavor, Hayashi et al disclose the use of a database to store the necessary information for authentication (see column 3, lines 7-33).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Dent et al with Hayashi et al to include the above storage of authorization information in order to avoid using the processing resources to compute the data.

Regarding **claim 8**, Dent et al disclose that after the base station authenticates the mobile station, the base station forms a response signal from a further random number RAND2 and form the personal identification number PIN of the mobile, this number being known in the base station and this is sent to the mobile station. The mobile station forms a value of RESP2 from its PIN and the received number RAND2 and compares this formed value with the received RESP2. If the two values coincide,

the method proceeds (see column 3, lines 4-34 and figure 2), which reads on the

claimed, "means for sending a mobile terminal a request signal requesting execution of

an operation... a receiver for receiving, from a mobile terminal that has received said

request signal requesting execution of the operation, an authentication request signal

that includes an identifier... of said mobile terminal," and, "an authentication operation

unit executes an authentication operation," and, "sending result of the authentication

operation to the mobile terminal." Dent et al fails to disclose the use of a table for

storing correspondence between an identifier and key information of a mobile terminal

and a key-information acquisition unit for acquiring key information, which corresponds

to the received identifier of the mobile terminal, from said table or the random number

being sent from the terminal.

In a similar field of endeavor, Hayashi et al disclose the use of a database to

store the necessary information for authentication (see column 3, lines 7-33) and a

random number generating unit at the mobile terminal.

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to modify Dent et al with Hayashi et al to include the above storage of

authorization information and random number generating unit at the mobile in order to

avoid using the processing resources to compute the data and generate and send

random numbers at the network.

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dent et al

in view of Rosenthal et al (US005737701).

Regarding **claim 3**, Dent et al disclose bi-directional authentication between a

mobile station and a base station, so that it is not only the base station that requires the

identity of the mobile station, but the mobile station that requires the identity of the base

station (see column 1, line 67 – column 2, line 7), which reads on the claimed, "mobile

terminal in a mobile communication system for authenticating a communicating party

when communication is performed between the mobile terminal and a device on the

side of a network." After the base station authenticates the mobile station, the base

station forms a response signal from a further random number RAND2 and form the

personal identification number PIN of the mobile, this number being known in the base

station and this is sent to the mobile station. The mobile station forms a value of

RESP2 from its PIN and the received number RAND2 and compares this formed value

with the received RESP2. If the two values coincide, the method proceeds (see column

3, lines 4-34 and figure 2), which reads on the claimed, "authentication processing

means which, when a request signal requesting operation execution is received from a

network device, is for executing authentication processing to check whether said

request signal is a request signal from an authorized network device; and operation

execution means for executing an operation that is in accordance with said request

signal only if authentication that the network device is an authorized network device is

obtained." Dent et al further disclose bi-directional authentication between a mobile

station and a base station, so that it is not only the base station that requires the identity

of the mobile station, but the mobile station that requires the identity of the base station

before a call is completed (see column 1, line 67 – column 2, line 7), which reads on the

claimed, "said authentication processing means executes authentication processing if a

request is one requiring authentication, and said operation execution means executes

the operation that is in accordance with said request signal if authentication that the

network device is an authorized network device is obtained." Dent et al fail to disclose

an authentication necessity table which indicates whether each request received from

the network device requires authentication and forgoing authentication processing if a

request is not one requiring authentication.

In a similar field of endeavor, Rosenthal et al disclose a table that can be

searched for instances where authentication is waived (see figure 3 and column 6, lines

20-28).

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to modify Dent et al with Rosenthal et al to include the above

authentication database in order to reduce the likelihood of communications fraud by

decreasing the exposure of the authentication code as suggested by Rosenthal et al

(see column 3, lines 52-57).

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dent et al

in view of Jiang et al (US 20020057678A1).

Regarding **claim 7**, Dent et al disclose bi-directional authentication between a

mobile station and a base station, so that it is not only the base station that requires the

identity of the mobile station, but the mobile station that requires the identity of the base

station (see column 1, line 67 – column 2, line 7), which reads on the claimed, "mobile

communication system for authenticating a communicating party when communication

is performed between a mobile terminal and a device on the side of a network." After

the base station authenticates the mobile station, the base station forms a response

signal from a further random number RAND2 and form the personal identification

number PIN of the mobile, this number being known in the base station and this is sent

to the mobile station. The mobile station forms a value of RESP2 from its PIN and the

received number RAND2 and compares this formed value with the received RESP2. If

the two values coincide, the method proceeds (see column 3, lines 4-34 and figure 2),

which reads on the claimed, "authentication processing means which, when a signal

requesting execution of a prescribed operation has been received from a network

device, is for sending an authentication request signal to the network device in order to

determine whether said request signal is a request signal from an authorized network

device; performing an authentication operation; and comparing result of this

authentication operation with result of an authentication operation sent from the network

device; and operation execution means for executing an operation that is in accordance

with said request signal only if authentication that the network device is an authorized

network device is obtained; and said network device includes an authentication

operation unit for executing an authentication operation based upon an authentication

request signal received from said mobile terminal based upon an authentication request

signal received from said mobile terminal, and sending result of this authentication

operation to the mobile terminal." Dent et al further disclose bi-directional authentication

between a mobile station and a base station, so that it is not only the base station that

requires the identity of the mobile station, but the mobile station that requires the identity

of the base station before a call is completed (see column 1, line 67 – column 2, line 7),

which reads on the claimed, "said authentication processing means executes

authentication processing if a request is one requiring authentication, and said operation

execution means executes the operation that is in accordance with said request signal if

authentication that the network device is an authorized network device is obtained."

Dent et al fail to expressly disclose forgoing authentication processing if a request is not

one requiring authentication.

In a similar field of endeavor, Jiang et al disclose skipping authentication if it is

not necessary for a particular application (see paragraph 208).

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to modify Dent et al with Jiang et al to include the above skipping

authentication when not necessary for an application in order to conserve system

resources.

Claims 9, 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Dent et al in view of Lipovski (US 20040087318A1).

Regarding **claim 9**, Dent et al disclose bi-directional authentication between a

mobile station and a base station, so that it is not only the base station that requires the

identity of the mobile station, but the mobile station that requires the identity of the base

station (see column 1, line 67 – column 2, line 7), which reads on the claimed, "mobile

communication system for authenticating a communicating party when communication

is performed between a mobile terminal and a device on the side of a network." After

the base station authenticates the mobile station, the base station forms a response

signal from a further random number RAND2 and form the personal identification

number PIN of the mobile, this number being known in the base station and this is sent

to the mobile station. The mobile station forms a value of RESP2 from its PIN and the

received number RAND2 and compares this formed value with the received RESP2. If

the two values coincide, the method proceeds (see column 3, lines 4-34 and figure 2),

which reads on the claimed, "authentication processing means which, when a signal

requesting execution of a prescribed operation has been received from a network

device, is for sending an authentication request signal to the network device in order to

determine whether said request signal is a request signal from an authorized network

device; performing an authentication operation; and comparing result of this

authentication operation with result of an authentication operation sent from the network

device; and operation execution means for executing an operation that is in accordance

with said request signal only if authentication that the network device is an authorized

network device is obtained; and said network device includes an authentication

operation unit for executing an authentication operation based upon an authentication

request signal received from said mobile terminal based upon an authentication request

signal received from said mobile terminal, and sending result of this authentication

operation to the mobile terminal." Dent et al fail to disclose the request signal

requesting operation execution is a signal requesting that emission of radio waves be

inhibited.

In a similar field of endeavor, Lipovski discloses a transmitter sending a signal requesting a terminal to mute radio frequency generation (see paragraph 20).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Dent et al with Lipovski to include the above signal muting radio frequency generation in order to automatically restrict devices where they would create a distraction or in airplanes (see paragraphs 3-4).

Regarding **claim 10**, Dent et al fail to disclose the request signal requesting operation execution is a signal requesting that inhibition of emission of radio waves be cancelled.

In a similar field of endeavor, Lipovski discloses a transmitter sending a signal requesting a terminal to mute radio frequency generation, then at the exit, another to allow transmission (see paragraph 20).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Dent et al with Lipovski to include the above signal muting radio frequency generation and allowance in order to automatically restrict devices where they would create a distraction or in airplanes (see paragraphs 3-4) and to provide minimum inconvenience to the user.

Regarding **claim 11**, Dent et al fail to disclose the request signal requesting operation execution is a signal requesting that the mobile station make a transmission to power cut-off or to a standby operation.

In a similar field of endeavor, Lipovski discloses a transmitter sending a signal requesting a terminal to mute radio frequency generation (see paragraph 20), which reads on the claimed, "standby operation."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Dent et al with Lipovski to include the above signal muting radio frequency generation in order to automatically restrict devices where they would create a distraction or in airplanes (see paragraphs 3-4).

Claims 12, 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dent et al in view of Durst et al (US 20030122707A1).

Regarding **claim 12**, Dent et al fail to disclose that the request signal requesting operation execution is a signal requesting disclosure of mobile terminal information possessed by the mobile terminal.

In a similar field of endeavor, Durst et al disclose a base station transmits a location information request to a mobile terminal and the terminal responds with current location information (see paragraph 39), which reads on the claimed, "said request signal requesting operation execution is a signal requesting disclosure of mobile terminal information possessed by the mobile terminal."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Dent et al with Durst et al to include the above location information update in order to assist the authorities in case of an emergency by providing the location of a user.

Regarding **claim 14**, Dent et al fail to disclose the mobile terminal information is status information of the mobile terminal.

In a similar field of endeavor, Durst et al disclose a base station transmits a location information request to a mobile terminal and the terminal responds with current location information (see paragraph 39), which reads on the claimed, "said mobile terminal information is status information of the mobile terminal."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Dent et al with Durst et al to include the above location information update in order to assist the authorities in case of an emergency by providing the location of a user.

Regarding **claim 15**, Dent et al fail to disclose the status information is voltage information indicating residual capacity of a battery of the terminal, or traveling-velocity information measured by a mobile unit, or present-position information detected by a mobile unit.

In a similar field of endeavor, Durst et al disclose a base station transmits a location information request to a mobile terminal and the terminal responds with current location information (see paragraph 39), which reads on the claimed, "said status information is voltage information indicating residual capacity of a battery of the terminal, or traveling-velocity information measured by a mobile unit, or present-position information detected by a mobile unit."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Dent et al with Durst et al to include the above location

information update in order to assist the authorities in case of an emergency by

providing the location of a user.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dent et

al in view of Durst et al, as applied to claim 12 above, and further in view of Mills

(US005915225A).

Regarding **claim 13**, the combination of Dent et al and Durst et al fails to

expressly disclose that the mobile terminal information is user settings information that a

user of the mobile terminal has stored beforehand in a storage unit of the mobile

terminal.

In a similar field of endeavor, Mills discloses a system that allows the mobile

telecommunications network to request and retrieve the desired subscriber information

stored in a SIM card via over-the-air connection-less signals (see column 5, lines 1-13).

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to modify the combination of Dent et al and Durst et al with Mills to include

the above network requesting subscriber information in order to eliminate the need for a

subscriber to verbally provide details or tediously enter a long series of numbers while

on the phone as suggested by Mills (see column 4, line 56 – column 5, line 13).

Response to Arguments

Applicant's arguments filed August 9, 2006 have been fully considered but they

are not persuasive.

Applicant's arguments with respect to claims1, 5, 8 and 11-15 have been considered but are moot in view of the new ground(s) of rejection.

The Applicant argues the combination of Dent et al and Rosenthal fails to disclose the authentication table in the mobile terminal and the mobile terminal judges, by reference to this table, whether a request signal received from the network device requires an authentication processing. The Examiner respectfully disagrees. While Rosenthal may disclose the table is at the network, when modifying the reference for the bilateral authentication of Dent et al, the table would have been added at the mobile station.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bryan J. Fox whose telephone number is (571) 272-7908. The examiner can normally be reached on Monday through Friday 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Feild can be reached on (571) 272-4090. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Bryan Fox
October 17, 2006

JOSEPH FEILD
SUPERVISORY PATENT EXAMINER